UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,853	03/18/2004	Shoji Kodama	274.43202X00	5857

24956 7590 12/29/2008

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
LEWIS, ALICIA M	

ART UNIT	PAPER NUMBER
2164	

MAIL DATE	DELIVERY MODE
12/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/802,853	KODAMA, SHOJI	
	Examiner	Art Unit	
	Alicia M. Lewis	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6,9-13,17,18,21-25 and 28-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,6,9-13,17,18,21-25 and 28-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is responsive to the Affidavit and Remarks filed on September 8, 2008. Claims 9, 11, 21, 22, 29 and 30 are presently amended, and claims 2-5, 7, 8, 14-16, 19, 20, 26, and 27 are canceled. Therefore, claims 1, 6, 9-13, 17, 18, 21-25 and 28-35 remain pending in this application.

Claim Objections

1. Claims 6, 9-12, 17-18, 21-24 and 28-32 are objected to because of the following informalities: the “a” at the beginning of the claim should be changed to “the" to show their dependence on corresponding independent claims. Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 25 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamamoto (US Patent Application Publication 2002/0152339 A1) in view of Chris Lueth, “WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise,” (published September 2003) (‘Lueth’).

With respect to claim 1, Yamamoto teaches a system for protecting data on a physical volume at the file system level and permitting access to the data at the physical volume level comprising:

a first interface for file level input/output (I/O) (paragraph 18 lines 1-5);

a second interface for block level I/O (paragraph 18 lines 1-4);

a plurality of physical volumes upon which file systems are represented (paragraphs 7-8, paragraphs 43-44);

a first controller which processes file level I/O requests (paragraph 7 lines 4-7 and 13-16); and

a second controller which processes block level I/O requests (paragraph 7 lines 4-5 and 13-16),

wherein, in response to a file system protect request directed to a particular file system, the particular file system is protected for a specified period of time and a physical volume of the particular file system is also protected for the specified period of time (paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39), and

wherein once the particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time (paragraphs 35, 39 and 47),

wherein information regarding whether or not the particular file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of the particular file system (Figures 5 and 6, paragraphs 43, 45 and 47).

Although Yamamoto uses the term a controller element, it is clear that there are two separate controller elements being used, one for file level and one for block level. For example, he states in paragraph 7 that the controller elements includes at least a SCSI interface for block type read/write requests and a file system interface for file level read/write requests. This interpretation is upheld throughout this office action wherever

Although it is inherent that if a file system or physical volume is protected at all, then it is protected for a specified period of time, Yamamoto does not explicitly recite a protect request directed to a file system with a specified period of time, nor does he teach wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system.

Lueth teaches WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise (see abstract), in which he teaches a protect request directed to a file system with a specified period of time (page 10, *Using Retention Dates with SnapLock Compliance* and Section 3.4.1); and a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the

particular file system (page 10, *Using Retention Dates with SnapLock Compliance* and Sections 3.4.1 and 3.4.2).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yamamoto by the teaching of Lueth because a protect request directed to a file system with a specified period of time and wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system would enable usage of WORM data storage to meet regulatory compliance and to add another layer to a business's data protection roadmap (Lueth, abstract).

With respect to claim 25, Yamamoto as modified teaches a storage system for protecting data on a physical volume at the file system level and permitting access to the data at the physical volume level comprising:

a first interface for file level input/output (I/O) (Yamamoto, paragraph 18 lines 1-5);

a second interface for block level I/O (Yamamoto, paragraph 18 lines 1-4);

a plurality of physical volumes upon which file systems are represented (Yamamoto, paragraphs 7 and 8, paragraphs 43-44);

a first controller which processes file level I/O requests (Yamamoto, paragraph 7 lines 4-7 and 13-16); and

a second controller which processes block level I/O requests (Yamamoto, paragraph 7 lines 4-5 and 13-16),

wherein, in response to a file system protect request directed to a particular file system with a specified period of time (Lueth, page 10, *Using Retention Dates with SnapLock Compliance* and Section 3.4.1), the particular file system is protected for the specified period of time and a physical volume of the particular file system is also protected for the specified period of time (Yamamoto, paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39),

wherein once the particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time (Yamamoto, paragraphs 35, 39 and 47),

wherein information regarding whether or not the particular file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of the particular file system (Yamamoto, Figures 5 and 6, paragraphs 43, 45 and 47), and

wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system (Lueth, page 10, *Using Retention Dates with SnapLock Compliance* and Sections 3.4.1 and 3.4.2).

With respect to claim 33, Yamamoto as modified teaches a storage system for handling input/output (I/O) requests from a plurality of servers, wherein a first server of the servers sends file I/O requests and a second server of the servers sends block I/O requests, comprising:

a storage media including a plurality of volumes (Yamamoto, paragraph 7 lines 1-2) storing data of file systems (Yamamoto, paragraph 8 lines 1-2);

a first controller, to be coupled to the first server, conducting I/O operations in response to the file I/O requests (Yamamoto, paragraph 7);

a second controller, coupled to the storage media, to be coupled to the second server, conducting I/O operations in response to the block I/O requests (Yamamoto, paragraph 7); and

wherein at least one file system of the file systems is set to be write-protected from the second controller when the first controller received a request from the first server to protect said at least one file system in the storage media for a specified period of time (Yamamoto, paragraphs 35-39 and 47; Lueth, page 10, *Using Retention Dates with SnapLock Compliance* and Section 3.4.1),

wherein information regarding whether or not said at least one file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of said at least one file system (Yamamoto, Figures 5 and 6, paragraphs 43, 45 and 47), and

wherein said entries include a first status indicating a retention period of said at least one file system, the retention period indicating how long data in said at least one

file system should remain unchanged and thereby determining when data can next be written to said at least one file system (Lueth, page 10, *Using Retention Dates with SnapLock Compliance* and Sections 3.4.1 and 3.4.2).

With respect to claim 34, Yamamoto as modified teaches wherein said first and second controllers share protection information (Yamamoto, paragraph 7 lines 13-16) including status of protection (Yamamoto, paragraph 47) and a retention period for each of the file systems which is set by the first controller (Lueth, page 10, *Using Retention Dates with SnapLock Compliance* and Sections 3.4.1 and 3.4.2).

With respect to claim 35, Yamamoto as modified teaches wherein the first controller receives the file I/O requests via a first interface and the second controller receives the block I/O requests via a second interface (Yamamoto, paragraphs 7 and 18).

4. Claims 6 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamamoto (US Patent Application Publication 2002/0152339 A1) in view of Chris Lueth, "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise," (published September 2003) ('Lueth'), as applied to claims 1, 25 and 33-35 above, and further in view of Brewer et al. (US Patent 6,336,163 B1) ('Brewer').

With respect to claims 6 and 28, Yamamoto as modified teaches claims 1 and 25 and entries indicating a status of a volume and/or file system.

Yamamoto as modified does not teach wherein said entries indicate a second status defining whether the file system is exported or un-exported.

Brewer teaches a method and article of manufacture for inserting volumes for import into a virtual tape server (see abstract), in which he teaches wherein said entries indicate a second status of each volume defining whether the volume is exported or un-exported (Brewer, column 2 lines 56-60, column 6 lines 24-26).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Yamamoto by the teaching of Brewer because wherein said entries indicate a second status of each volume defining whether the volume is exported or un-exported would enable a more detailed tracking of all types of volumes, not just file systems, which would add functionality to Yamamoto's storage system (Brewer, column 6 lines 1-3).

5. Claims 9-12 and 29, 31, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamamoto (US Patent Application Publication 2002/0152339 A1) in view of Chris Lueth, "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise," (published September 2003) ('Lueth'), as applied to claims 1, 25 and 33-35 above, and further in view of Achiwa et al. (US Patent Application Publication 2003/0009438 A1) ('Achiwa').

With respect to claims 9 and 29, Yamamoto as modified teaches wherein in response to said file system protect request, said first controller sets the information corresponding to said specified period of time to said particular file system and sets the information corresponding to said specified period of time to said physical volume of said particular file system (Yamamoto, paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39; Lueth, Lueth, page 10, *Using Retention Dates with SnapLock Compliance* and Sections 3.4.1 and 3.4.2).

Yamamoto as modified does not teach wherein said first controller is a network attached storage controller which processes file level I/O requests.

Achiwa teaches a method for file level remote copy of a storage device (see abstract) in which he teaches wherein said first controller is a network attached storage controller which processes file level I/O requests (paragraph 38).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Yamamoto by the teaching of Achiwa because wherein said first controller is a network attached storage controller which processes file level I/O requests would enable processing of file or directory level access requests (Achiwa, paragraph 8).

With respect to claim 10, Yamamoto as modified teaches wherein said second controller is a disk controller which processes block level I/O requests (Achiwa, paragraph 93).

With respect to claim 11, Yamamoto as modified teaches wherein said first interface is an Ethernet interface which processes file level I/O requests (Achiwa, paragraph 96), and

wherein in response to a file system delete request, said first controller checks a status of a specified file system and statuses of each corresponding physical volume of said file system (Yamamoto, paragraph 45; Lueth, page 10, Sections 3.4.1 and 3.4.2), and if shredding is required, said first controller deletes all the data on each corresponding physical volume by shredding.

The last limitation, "if shredding is required, said first controller deletes all the data on each corresponding physical volume by shredding" is optionally recited and thus holds no patentable weight. The deletion by shredding only occurs if it is determined that shredding is required.

With respect to claims 12 and 32, Yamamoto as modified teaches wherein said second interface is a Fibre Channel interface which processes block level I/O requests (Achiwa, paragraph 93, paragraph 98).

With respect to claim 31, Yamamoto as modified teaches wherein said first interface is an Ethernet interface which processes file level I/O requests (Achiwa, paragraph 96).

6. Claims 13, 17 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoogterp (US Patent Application Publication 2005/0210218 A1) in view of Yamamoto (US Patent Application Publication 2002/0152339 A1), and further in view of Chris Lueth, "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise," (published September 2003) ('Lueth').

With respect to claim 13, Hoogterp teaches a storage system for protecting data on a physical volume at the file system level and permitting access to the data at the physical volume level comprising:

a network attached storage (NAS) gateway (Figure 4, paragraphs 27 and 52); and

a storage system which is connected to said NAS gateway (Figure 4, paragraphs 52 and 55),

wherein said NAS gateway comprises:

a first interface for file level I/O (element 168 in Figure 4, paragraph 52);

a third interface for block level I/O (element 169 in Figure 4, paragraphs 52-54), and

a first controller which processes file level I/O requests (paragraph 56);

wherein said storage system comprises:

a second interface for block level I/O, said second interface being connected to said third interface (paragraph 34),

a plurality of physical volumes upon which file systems are represented (paragraphs 58 and 62);

a second controller which processes block level I/O requests (paragraph 34); and

wherein once a particular logical volume is protected, write requests to the particular logical volume or physical volume of the particular logical volume via either the first or second controller are not permitted until expiration of the specified period of time (paragraph 150).

Hoogterp does not explicitly teach wherein, in response to a file system protect request directed to a particular file system with a specified period of time, the particular file system is protected for the specified period of time and a physical volume of the particular file system is also protected for the specified period of time; or wherein once a particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time.

Yamamoto teaches a direct access storage system with combined block interface and file interface access (see abstract), in which he teaches:

a first interface for file level input/output (I/O) (paragraph 18 lines 1-5);

a second interface for block level I/O (paragraph 18 lines 1-4);

a plurality of physical volumes upon which file systems are represented (paragraphs 7-8, paragraphs 43-44);

a first controller which processes file level I/O requests (paragraph 7 lines 4-7 and 13-16); and

a second controller which processes block level I/O requests (paragraph 7 lines 4-5 and 13-16),

wherein, in response to a file system protect request directed to a particular file system, the particular file system is protected for a specified period of time and a physical volume of the particular file system is also protected for the specified period of time (paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39), and

wherein once the particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time (paragraphs 35, 39 and 47),

wherein information regarding whether or not the particular file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of the particular file system (Figures 5 and 6, paragraphs 43, 45 and 47).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoogterp by the teaching of Yamamoto because wherein said first and second controllers share protection information for said logical and physical volumes would enable a storage system with direct access storage devices that could be shared between a block interface and a file interface (Yamamoto, paragraph 6).

Further regarding claim 13, the combination of Hoogterp and Yamamoto does not teach a protect request directed to a file system with a specified period of time or wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system.

Lueth teaches WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise (see abstract), in which he teaches a protect request directed to a file system with a specified period of time (page 10, *Using Retention Dates with SnapLock Compliance* and Section 3.4.1); and a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system (page 10, *Using Retention Dates with SnapLock Compliance* and Sections 3.4.1 and 3.4.2).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Hoogterp by the teaching of Lueth because a protect request directed to a file system with a specified period of time and wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system would enable usage of WORM data storage to meet regulatory

compliance and to add another layer to a business's data protection roadmap (Lueth, abstract).

With respect to claim 17, Hoogterp as modified teaches wherein said entries indicate a second status of each file system defining whether the file system is protected or unprotected (Yamamoto, paragraph 47).

With respect to claim 24, Hoogterp as modified teaches wherein said second interface is a Fibre Channel interface which processes block level I/O requests (Hoogterp, paragraph 34).

7. Claims 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hoogterp (US Patent Application Publication 2005/0210218 A1) in view of Yamamoto (US Patent Application Publication 2002/0152339 A1) and Chris Lueth, "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise," (published September 2003) ('Lueth'), as applied to claims 13, 17 and 24 above, and further in view of Brewer et al. (US Patent 6,336,163 B1) ('Brewer').

With respect to claim 18, Hoogterp as modified teaches claim 13.

Hoogterp as modified does not teach a second status of each file system defining whether the file system is exported or un-exported (Brewer, column 2 lines 56-60, column 6 lines 24-26).

Brewer teaches a method and article of manufacture for inserting volumes for import into a virtual tape server (see abstract), in which he teaches wherein said entries indicate a second status of each volume defining whether the volume is exported or un-exported (Brewer, column 2 lines 56-60, column 6 lines 24-26).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Hoogterp by the teaching of Brewer because a second status of each volume defining whether the file system is exported or un-exported would enable a more detailed tracking of all types of volumes, not just file systems, which would add functionality to Hoogterp's system (Brewer, column 6 lines 1-3).

8. Claims 21 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoogterp (US Patent Application Publication 2005/0210218 A1) in view of Yamamoto (US Patent Application Publication 2002/0152339 A1) and Chris Lueth, "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise," (published September 2003) ('Lueth'), as applied to claims 13, 17 and 24 above, and further in view of Achiwa et al. (US Patent Application Publication 2003/0009438 A1) ('Achiwa').

With respect to claim 21, Hoogterp as modified teaches wherein in response to said file system protect request, said first controller sets the information corresponding to said specified period of time to said particular file system and sets the information

corresponding to said specified period of time to said physical volume of said particular file system (Yamamoto, paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39; Lueth, Lueth, page 10, *Using Retention Dates with SnapLock Compliance* and Sections 3.4.1 and 3.4.2).

Hoogterp as modified does not teach wherein said first controller is a network attached storage controller which processes file level I/O requests.

Achiwa teaches a method for file level remote copy of a storage device (see abstract) in which he teaches wherein said first controller is a network attached storage controller which processes file level I/O requests (paragraph 38).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Hoogterp by the teaching of Achiwa because wherein said first controller is a network attached storage controller which processes file level I/O requests would enable processing of file or directory level access requests (Achiwa, paragraph 8).

With respect to claim 23, Hoogterp as modified teaches wherein said first interface is an Ethernet interface which processes file level I/O requests (Achiwa, paragraph 96).

9. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hoogterp (US Patent Application Publication 2005/0210218 A1) in view of Yamamoto

(US Patent Application Publication 2002/0152339 A1), Chris Lueth, "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise," (published September 2003) ('Lueth') and Achiwa et al. (US Patent Application Publication 2003/0009438 A1) ('Achiwa'), as applied to claims 21 and 23 above, and further in view of Reynolds (US 2002/0055942 A1).

With respect to claim 22, Hoogterp as modified teaches wherein said second controller is a disk controller which processes block level I/O requests (Achiwa, paragraph 93), and wherein in response to a file system delete request, said first controller checks a status of a specified file system and statuses of each corresponding physical volume of said file system (Yamamoto, paragraph 45; Lueth, page 10, Sections 3.4.1 and 3.4.2).

Hoogterp as modified does not teach, if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool.

Reynolds teaches creating, verifying, managing, and using original digital files (see abstract), in which he teaches if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool (paragraph 60).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Hoogterp by the teaching of Reynolds because if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool would enable secure deletion of secure data files (Reynolds, paragraph 60).

10. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamamoto (US Patent Application Publication 2002/0152339 A1) in view of Chris Lueth, "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise," (published September 2003) ('Lueth') and Achiwa et al. (US Patent Application Publication 2003/0009438 A1) ('Achiwa'), as applied to claims 9-12 and 29, 31, 32 above, and further in view of Reynolds (US 2002/0055942 A1).

With respect to claim 30, Yamamoto as modified teaches wherein said second controller is a disk controller which processes block level I/O requests (Achiwa, paragraph 93), and wherein in response to a file system delete request, said first controller checks a status of a specified file system and statuses of each corresponding physical volume of said file system (Yamamoto, paragraph 45; Lueth, page 10, Sections 3.4.1 and 3.4.2).

Yamamoto as modified does not teach, if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and

if a shredding is not required said first controller places each corresponding physical volume to a free volume pool.

Reynolds teaches creating, verifying, managing, and using original digital files (see abstract), in which he teaches if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool (paragraph 60).

11. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Yamamoto by the teaching of Reynolds because if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool would enable secure deletion of secure data files (Reynolds, paragraph 60).

12. Claims 1, 11, 25 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamamoto (US Patent Application Publication 2002/0152339 A1) in view of Stakutis et al. (US 2006/0282484 A1) ('Stakutis').

With respect to claim 1, Yamamoto teaches a system for protecting data on a physical volume at the file system level and permitting access to the data at the physical volume level comprising:

a first interface for file level input/output (I/O) (paragraph 18 lines 1-5);

a second interface for block level I/O (paragraph 18 lines 1-4);

a plurality of physical volumes upon which file systems are represented (paragraphs 7-8, paragraphs 43-44);

a first controller which processes file level I/O requests (paragraph 7 lines 4-7 and 13-16); and

a second controller which processes block level I/O requests (paragraph 7 lines 4-5 and 13-16),

wherein, in response to a file system protect request directed to a particular file system, the particular file system is protected for a specified period of time and a physical volume of the particular file system is also protected for the specified period of time (paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39), and

wherein once the particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time (paragraphs 35, 39 and 47),

wherein information regarding whether or not the particular file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of the particular file system (Figures 5 and 6, paragraphs 43, 45 and 47).

Although Yamamoto uses the term a controller element, it is clear that there are two separate controller elements being used, one for file level and one for block level. For example, he states in paragraph 7 that the controller elements includes at least a

SCSI interface for block type read/write requests and a file system interface for file level read/write requests. This interpretation is upheld throughout this office action wherever

Although it is inherent that if a file system or physical volume is protected at all, then it is protected for a specified period of time, Yamamoto does not explicitly recite a protect request directed to a file system with a specified period of time, nor does he teach wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system.

Stakutis teaches a method, system and program for archiving files (see abstract), in which he teaches a protect request directed to a file system with a specified period of time (paragraphs 22-24); and a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system (paragraph 22).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Yamamoto by the teaching of Stakutis because a protect request directed to a file system with a specified period of time and wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the

particular file system would enable an efficient archival retention policy for a file system (Stakutis, abstract).

With respect to claim 11, Yamamoto as modified teaches wherein said first interface is an Ethernet interface which processes file level I/O requests (Stakutis, paragraph 21), and

wherein in response to a file system delete request, said first controller checks a status of a specified file system and statuses of each corresponding physical volume of said file system (Stakutis, Figure 4, paragraphs 29-31) and if shredding is required, said first controller deletes all the data on each corresponding physical volume by shredding.

The last limitation, "if shredding is required, said first controller deletes all the data on each corresponding physical volume by shredding" is optionally recited and thus holds no patentable weight. The deletion by shredding only occurs if it is determined that shredding is required.

With respect to claim 25, Yamamoto as modified teaches a storage system for protecting data on a physical volume at the file system level and permitting access to the data at the physical volume level comprising:

a first interface for file level input/output (I/O) (Yamamoto, paragraph 18 lines 1-5);

a second interface for block level I/O (Yamamoto, paragraph 18 lines 1-4);

a plurality of physical volumes upon which file systems are represented (Yamamoto, paragraphs 7 and 8, paragraphs 43-44);

a first controller which processes file level I/O requests (Yamamoto, paragraph 7 lines 4-7 and 13-16); and

a second controller which processes block level I/O requests (Yamamoto, paragraph 7 lines 4-5 and 13-16),

wherein, in response to a file system protect request directed to a particular file system with a specified period of time (Stakutis, paragraphs 22-24), the particular file system is protected for the specified period of time and a physical volume of the particular file system is also protected for the specified period of time (Yamamoto, paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39),

wherein once the particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time (Yamamoto, paragraphs 35, 39 and 47),

wherein information regarding whether or not the particular file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of the particular file system (Yamamoto, Figures 5 and 6, paragraphs 43, 45 and 47), and

wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file

system should remain unchanged and thereby determining when data can next be written to the particular file system (Stakutis, paragraph 22).

With respect to claim 33, Yamamoto as modified teaches a storage system for handling input/output (I/O) requests from a plurality of servers, wherein a first server of the servers sends file I/O requests and a second server of the servers sends block I/O requests, comprising:

a storage media including a plurality of volumes (Yamamoto, paragraph 7 lines 1-2) storing data of file systems (Yamamoto, paragraph 8 lines 1-2);

a first controller, to be coupled to the first server, conducting I/O operations in response to the file I/O requests (Yamamoto, paragraph 7);

a second controller, coupled to the storage media, to be coupled to the second server, conducting I/O operations in response to the block I/O requests (Yamamoto, paragraph 7); and

wherein at least one file system of the file systems is set to be write-protected from the second controller when the first controller received a request from the first server to protect said at least one file system in the storage media for a specified period of time (Yamamoto, paragraphs 35-39 and 47; Stakutis, paragraphs 22-24),

wherein information regarding whether or not said at least one file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of said at least one file system (Yamamoto, Figures 5 and 6, paragraphs 43, 45 and 47), and

wherein said entries include a first status indicating a retention period of said at least one file system, the retention period indicating how long data in said at least one file system should remain unchanged and thereby determining when data can next be written to said at least one file system (Stakutis, paragraph 22).

With respect to claim 34, Yamamoto as modified teaches wherein said first and second controllers share protection information (Yamamoto, paragraph 7 lines 13-16) including status of protection (Yamamoto, paragraph 47) and a retention period for each of the file systems which is set by the first controller (Stakutis, paragraph 22).

With respect to claim 35, Yamamoto as modified teaches wherein the first controller receives the file I/O requests via a first interface and the second controller receives the block I/O requests via a second interface (Yamamoto, paragraphs 7 and 18).

13. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hoogterp (US Patent Application Publication 2005/0210218 A1) in view of Yamamoto (US Patent Application Publication 2002/0152339 A1), and further in view of Stakutis et al. (US 2006/0282484 A1) ('Stakutis').

With respect to claim 13, Hoogterp teaches a storage system for protecting data on a physical volume at the file system level and permitting access to the data at the physical volume level comprising:

a network attached storage (NAS) gateway (Figure 4, paragraphs 27 and 52); and

a storage system which is connected to said NAS gateway (Figure 4, paragraphs 52 and 55),

wherein said NAS gateway comprises:

a first interface for file level I/O (element 168 in Figure 4, paragraph 52);

a third interface for block level I/O (element 169 in Figure 4, paragraphs 52-54), and

a first controller which processes file level I/O requests (paragraph 56);

wherein said storage system comprises:

a second interface for block level I/O, said second interface being connected to said third interface (paragraph 34),

a plurality of physical volumes upon which file systems are represented (paragraphs 58 and 62);

a second controller which processes block level I/O requests (paragraph 34); and

wherein once a particular logical volume is protected, write requests to the particular logical volume or physical volume of the particular logical volume via either

the first or second controller are not permitted until expiration of the specified period of time (paragraph 150).

Hoogterp does not explicitly teach wherein, in response to a file system protect request directed to a particular file system with a specified period of time, the particular file system is protected for the specified period of time and a physical volume of the particular file system is also protected for the specified period of time; or wherein once a particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time.

Yamamoto teaches a direct access storage system with combined block interface and file interface access (see abstract), in which he teaches:

a first interface for file level input/output (I/O) (paragraph 18 lines 1-5);

a second interface for block level I/O (paragraph 18 lines 1-4);

a plurality of physical volumes upon which file systems are represented (paragraphs 7-8, paragraphs 43-44);

a first controller which processes file level I/O requests (paragraph 7 lines 4-7 and 13-16); and

a second controller which processes block level I/O requests (paragraph 7 lines 4-5 and 13-16),

wherein, in response to a file system protect request directed to a particular file system, the particular file system is protected for a specified period of time and a

physical volume of the particular file system is also protected for the specified period of time (paragraph 6, paragraph 7 lines 13-16, paragraph 35, paragraph 39), and

wherein once the particular file system is protected, write requests to the particular file system or physical volume of the particular file system via either the first or second controller are not permitted until expiration of the specified period of time (paragraphs 35, 39 and 47),

wherein information regarding whether or not the particular file system is protected is stored in a volume status table having a plurality of entries which indicate statuses of the particular file system (Figures 5 and 6, paragraphs 43, 45 and 47).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoogterp by the teaching of Yamamoto because wherein said first and second controllers share protection information for said logical and physical volumes would enable a storage system with direct access storage devices that could be shared between a block interface and a file interface (Yamamoto, paragraph 6).

Further regarding claim 13, the combination of Hoogterp and Yamamoto does not teach a protect request directed to a file system with a specified period of time or wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system.

Stakutis teaches a method, system and program for archiving files (see abstract), in which he teaches a protect request directed to a file system with a specified period of time (paragraphs 22-24); and a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system (paragraph 22).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Hoogterp by the teaching of Stakutis because a protect request directed to a file system with a specified period of time and wherein said entries include a first status indicating a retention period for the particular file system, the retention period indicating how long data in the particular file system should remain unchanged and thereby determining when data can next be written to the particular file system would enable an efficient archival retention policy for a file system (Stakutis, abstract).

14. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hoogterp (US Patent Application Publication 2005/0210218 A1) in view of Yamamoto (US Patent Application Publication 2002/0152339 A1), Stakutis et al. (US 2006/0282484 A1) ('Stakutis') and Achiwa et al. (US Patent Application Publication 2003/0009438 A1) ('Achiwa'), and further in view of Reynolds (US 2002/0055942 A1).

With respect to claim 22, Hoogterp in view of Yamamoto and Stakutis teaches and wherein in response to a file system delete request, said first controller checks a status of a specified file system and statuses of each corresponding physical volume of said file system (Stakutis, Figure 4, paragraphs 29-31).

Hoogterp in view of Yamamoto and Stakutis does not teach wherein said second controller is a disk controller which processes block level I/O requests.

Achiwa teaches Achiwa teaches a method for file level remote copy of a storage device (see abstract) in which he teaches wherein said second controller is a disk controller which processes block level I/O requests (paragraph 93).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Hoogterp by the teaching of Achiwa because wherein said second controller is a disk controller which processes block level I/O requests would enable processing of file or directory level access requests (Achiwa, paragraph 8).

Further regarding claim 22, Hoogterp in view of Yamamoto and Stakutis does not teach, if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool.

Reynolds teaches creating, verifying, managing, and using original digital files (see abstract), in which he teaches if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is

not required said first controller places each corresponding physical volume to a free volume pool (paragraph 60).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Hoogterp by the teaching of Reynolds because if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool would enable secure deletion of secure data files (Reynolds, paragraph 60).

15. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamamoto (US Patent Application Publication 2002/0152339 A1) in view of Stakutis et al. (US 2006/0282484 A1) ('Stakutis') and Achiwa et al. (US Patent Application Publication 2003/0009438 A1) ('Achiwa'), and further in view of Reynolds (US 2002/0055942 A1).

With respect to claim 30, Yamamoto in view of Stakutis teaches claim 25 and wherein in response to a file system delete request, said first controller checks a status of a specified file system and statuses of each corresponding physical volume of said file system (Stakutis, Figure 4, paragraphs 29-31).

Yamamoto in view of Stakutis does not teach wherein said second controller is a disk controller which processes block level I/O requests.

Achiwa teaches Achiwa teaches a method for file level remote copy of a storage device (see abstract) in which he teaches wherein said second controller is a disk controller which processes block level I/O requests (paragraph 93).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Yamamoto by the teaching of Achiwa because wherein said second controller is a disk controller which processes block level I/O requests would enable processing of file or directory level access requests (Achiwa, paragraph 8).

Further regarding claim 30, Yamamoto in view of Stakutis and Achiwa does not teach if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool.

Reynolds teaches creating, verifying, managing, and using original digital files (see abstract), in which he teaches if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required said first controller places each corresponding physical volume to a free volume pool (paragraph 60).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have further modified Yamamoto by the teaching of Reynolds because if a shredding is required said first controller deletes all the data on each corresponding physical volume by shredding, and if a shredding is not required

said first controller places each corresponding physical volume to a free volume pool would enable secure deletion of secure data files (Reynolds, paragraph 60).

Response to Arguments

16. Applicant's arguments with respect to claims 1, 6, 9-13, 17, 18, 21-25 and 28-35 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Alicia M. Lewis whose telephone number is 571-272-5599. The examiner can normally be reached on Monday - Friday, 9 - 6:30, alternate Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on 571-272-4085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A. M. L./
Examiner, Art Unit 2164
December 12, 2008

/Charles Rones/
Supervisory Patent Examiner, Art Unit 2164